



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/827,082	04/19/2004	Christopher G. Kaler	13768.506	1874

22913 7590 12/26/2007
WORKMAN NYDEGGER
60 EAST SOUTH TEMPLE
1000 EAGLE GATE TOWER
SALT LAKE CITY, UT 84111

EXAMINER

ZEE, EDWARD

ART UNIT PAPER NUMBER

2135

MAIL DATE DELIVERY MODE

12/26/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

DETAILED ACTION

1. This is in response to the election to restriction filed on October 26th, 2007. Claims 1, 2, 4, 8, 9, 11-13, 21, 32 and 33 have been amended; Claims 14-20 and 31 have been cancelled; Claims 1-13, 21-30, 32 and 33 are pending and have been considered below.

Election/Restrictions

2. Applicant's election without traverse of Invention I (claims 1-13, 21-30, 32 and 33) in the reply filed on October 26th, 2007 is acknowledged.
3. Applicant is reminded that upon the cancellation of claims to a non-elected invention, the inventorship must be amended in compliance with 37 CFR 1.48(b) if one or more of the currently named inventors is no longer an inventor of at least one claim remaining in the application. Any amendment of inventorship must be accompanied by a request under 37 CFR 1.48(b) and by the fee required under 37 CFR 1.17(i).

Claim Objections

4. The amendments filed on August 3rd, 2007 have been considered and effectively overcome the previous claim objections. Therefore, the previous claim objections have been withdrawn.

Claim Rejections - 35 USC § 101

5. The amendments filed on August 3rd, 2007 have been considered and effectively overcome the previous 35 U.S.C. 101 claim rejections. Therefore, the previous claim rejections have been withdrawn.

Claim Rejections - 35 USC § 102

6. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

7. **Claims 1, 3-5, 8, 10, 11, 21-30, 32 and 33 are rejected under 35 U.S.C. 102(b) as being anticipated by Traw et al. (6,542,610).**

Claim 1: Traw et al. discloses a method for providing information that can be used to verify measurable aspects of a requesting computing system, the method comprising:

- a. determining that the providing computing system(*Device A*) is appropriately configured to issue challenges to components included in the requesting computing system(*Device B*) and determining that the providing application is appropriately configured to issue challenges to the requesting instructions(*Device A sends a challenge to Device B and compares the response to an expected value*) [column 7, lines 16-41];
- b. receiving a challenge initiated by the providing application based at least in part on the providing computing system and the providing application(*following successful completion of the preliminary authentication procedure, each device calculates and exchanges signed messages*), the challenge including information indicating how the requesting computing system is to prove that the requesting computing system is appropriately configured to access a

resource(*ie. device certificates typically contain a description of the ciphers that are supported by the device and may specify a key length and type of cipher to use*) [column 8, lines 33-39 | column 5, lines 1-10];

c. formulating proof, based on a measurable aspect of the requesting computing system's configuration, that the measurable aspect of the requesting computing system's configuration is appropriate for accessing a resource(*ie. formulating a response to a challenge with the appropriate key length and type of cipher as defined in the device certificate contained in the challenge*) [column 5, lines 1-10];

d. and submitting an assertion that can be used to verify that the requesting computing system is appropriately configured to access a resource(*signed messages*) [column 8, lines 33-39].

Claim 3: Traw et al. discloses a method as in claim 1 above and further discloses that the act of determining that the providing application is appropriately configured to issue challenges to the requesting instructions comprises receiving proof that the providing application complies with one or more security and trust policies of the requesting computing system(*compares data string to expected value to determine if devices can exchange protect content*) [column 7, lines 16-41].

Claim 4: Traw et al. discloses a method as in claim 1 above and further discloses that receiving a challenge that was initiated by the providing application comprises receiving a request for proof of the values(*signed message*) of one or more measurable aspects of the requesting computer system(*Device B transmits signed message to Device A*) [column 8, lines 33-39]. The examiner notes that the act of transmitting a proof value to Device A implies that Device B has accepted a request for a proof value.

Claim 5: Traw et al. discloses a method as in claim 1 above and further discloses that the submitted assertion includes the values of one or more measurable aspects of the requesting computer system(*signed message contains random challenge and Diffie-Hellman key exchange value*) [column 8, lines 33-39].

Claim 8: Traw et al. discloses a method for verifying measurable aspects of the requesting computing system, the method comprising:

a. proving that the providing computing system(*Device A*) is appropriately configured to issue challenges to components of the requesting computing system(*Device B*) (*each device verifies that the appropriate response has been received*) [column 7, lines 16-41];

b. causing a configuration challenge to be issued to the requesting instructions(*following successful completion of the preliminary authentication procedure, each device calculates and exchanges signed messages*), the challenge including information indicating how the requesting computing system is to prove that the requesting computing system is appropriately configured to access a resource(*ie. device certificates typically contain a description of the ciphers that are supported by the device and may specify a key length and type of cipher to use*) [column 8, lines 33-39 | column 5, lines 1-10];

c. receiving an assertion that can be used to verify that the requesting instructions are configured appropriately for interacting with the providing application(*signed messages*), the assertion including information based at least in part upon both a measurable aspect of the requesting system is configured and the information indicating how the requesting computing system is to prove that the requesting computing system is appropriately configured(*ie. formulating a response to a challenge with the appropriate key length and type of cipher as*

defined in the device certificate contained in the challenge) [column 8, lines 33-39 | column 5, lines 1-10].

Claim 10: Traw et al. discloses a method as in claim 8 above and further discloses that the act of proving that the providing application is appropriately configured to issue challenges to the requesting instructions comprises an act of sending proof(*data string*) that the providing application complies with one or more security and trust policies of the requesting computing system(*compares data string to expected value to determine if devices can exchange protect content*) [column 7, lines 16-41].

Claim 11: Traw et al. discloses a method as in claim 8 above and further discloses that causing a challenge to be issued to the requesting computing system comprises an act of requesting proof of the values of one or more measurable aspects of the requesting computer system(*signed message contains random challenge and Diffie-Hellman key exchange value*) [column 8, lines 33-39].

Claims 21 and 32: Traw et al. discloses a method and computer program-product for authorizing the requester to interact with the provider, the method comprising:

- a. sending a request to the provider(*devices exchange challenges*) [column 7, lines 6-15];
- b. receiving a configuration challenge from the provider, the configuration challenge including information indicating how the requester is to prove that the requester is appropriately configured to interact with the provider(*ie. device certificates typically contain a description of the ciphers that are supported by the device and may specify a key length and type of cipher to use*) [column 5, lines 1-10];

c. formulating proof, based on a measurable aspect of the requester's configuration, that the measurable aspect of the requesting computing system's configuration is appropriate for accessing a resource(*ie. formulating a response to a challenge with the appropriate key length and type of cipher as defined in the device certificate contained in the challenge*) [column 5, lines 1-10];

d. sending proof(*response*) of the values of one or more measurable aspects of the requester to the provider [column 7, lines 6-15];

e. receiving a token(*control channel key*) that can be used to prove that the requester is appropriately configured [column 7, lines 42-55].

Claim 22: Traw et al. discloses a method as in claim 21 above and further discloses that the act of sending a request to the provider comprises an act of sending a challenge along with the request, the challenge indicating how the provider is to prove that the provider is appropriately configured to issue configuration challenges to the requester(*devices exchange challenges*) [column 7, lines 6-15].

Claim 23: Traw et al. discloses a method as in claim 21 above and further discloses that the act of receiving a configuration challenge from the provider comprises an act receiving a configuration challenge along with proof(*response*) that the provider is appropriately configured to issue configuration challenges to the requester [column 7, lines 6-15].

Claim 24: Traw et al. discloses a method as in claim 21 above and further discloses that the act of sending proof(*response*) of the values of one or more measurable aspects of the requester to the provider comprises an act of sending a challenge along with the proof(*response*) of the values of one or more measurable aspects, the challenge indicating how the provider is to prove that the

provider is appropriately configured to issue configuration challenges to the requester(*devices exchange challenges*) [column 7, lines 6-15].

Claim 25: Traw et al. discloses a method as in claim 21 above and further discloses an act of receiving a token comprises an act of receiving a token(*control channel key*) along with proof(*response*) that the provider is appropriately configured to issue configuration challenges to the requester [column 7, lines 6-15 & lines 42-55].

Claims 26 and 33: Traw et al. discloses a method and computer program product for authorizing the requester and the provider to interact with the provider, the method comprising:

- a. an act of receiving a request from the requester(*devices exchange challenges*) [column 7, lines 6-15];
- b. an act of causing a configuration challenge to be issued to the requester, the configuration challenge requesting proof that the requester is appropriately configured to interact with the provider(*devices exchange challenges*) [column 7, lines 6-15];
- c. an act of receiving proof(*response*) of the values of one or more measurable aspects of the requester's configuration [column 7, lines 6-15];
- d. and an act of sending a token(*control channel key*) that can subsequently be used to prove that the requester is appropriately configured [column 7, lines 42-55].

Claim 27: Traw et al. discloses a method as in claim 26 above and further discloses that the act of receiving a request comprises an act of receiving a challenge along with the request, the challenge requesting proof that the provider is appropriately configured to issue configuration challenges to the requester(*devices exchange challenges*) [column 7, lines 6-15].

Claim 28: Traw et al. discloses a method as in claim 26 above and further discloses that the act of causing a configuration challenge to be issued to the requester comprises an act of sending a configuration challenge along with proof(*response*) that the provider is appropriately configured to issue configuration challenges to the requester(*devices exchange challenges*) [column 7, lines 6-15].

Claim 29: Traw et al. discloses a method as in claim 26 above and further discloses that the act of receiving proof of the values of one or more measurable aspects of the requester's configuration comprises an act of receiving a challenge along with the proof(*response*) of the values of the one or more measurable aspects, the challenge requesting proof that the provider is appropriately configured to issue configuration challenges to the requester(*devices exchange challenges*) [column 7, lines 6-15].

Claim 30: Traw et al. discloses a method as in claim 26 above and further discloses that the act of sending a token comprises sending a token(*control channel key*) along with proof(*response*) that the provider is appropriately configured to issue configuration challenges to the requester [column 7, lines 6-15 & lines 42-55].

Claim Rejections - 35 USC § 103

8. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

9. **Claims 2, 6, 7, 9 and 12-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Traw et al. (6,542,610).**

Claims 2 and 9: Traw et al. discloses a method as in claims 1 and 8 above, but does not explicitly disclose determining that the providing computing system is appropriately configured to issue challenges to components included in the requesting computing system comprises an act of establishing an SSL connection between the requesting computing system and the providing computer system. However, it would have been obvious to one of ordinary skill in the art at the time of invention to employ an SSL connection or any other form of secure connection between two computers when transmitting sensitive data across a network. One would have been motivated to do so in order to increase the integrity of the system.

Claims 6, 7, 12 and 13: Traw et al. discloses a method as in claims 1 and 8 above and further discloses that the exchanged device certificates can provide property information about the devices being authenticated [column 8, lines 18-20], but does not explicitly disclose that the submitted assertion indicates either the identity of one or more portions of the requesting instructions or the execution environment, nor that the act of receiving proof that the requesting instructions are appropriately configured for accessing the resource comprises an act of receiving proof of the values of either the identity of one or more portions of the requesting instructions or measurable aspects of the execution environment. However, it would have been obvious to one of ordinary skill in the art at the time of invention to identify the requesting instruction or execution environment as property information about the device being authenticated and furthermore receive proof of the identity or execution environment determine if the requesting instruction is appropriately configured. One would have been motivated to do so in order to increase the security of the authentication by employing a more comprehensive verification scheme.

Response to Arguments

10. Applicant's arguments filed August 3rd, 2007 have been fully considered but they are not persuasive.

Regarding Claim 1: The Applicant argues that the Traw et al. reference does not disclose a challenge which includes information indicating how the requesting computing system is to prove that it is appropriately configured to access a resource.

However, the Examiner respectfully disagrees and submits that Traw et al. does in fact disclose this feature. Traw et al. discloses that a "challenge" is generated from a random value and device certificate, wherein the device certificate may contain instructions specifying a key length or type of cipher to use [column 5, lines 1-10 | column 7, lines 16-21].

The Applicant further argues that the Traw et al. reference fails to teach that the requesting computing system formulates proof, based upon a measurable aspect of a system's configuration because the random challenge was supplied by another system and the encryption is performed based upon a hash algorithm independent of the system's configuration.

However, the Examiner respectfully disagrees and submits that in light of the argument presented above, Traw et al. does in fact disclose this feature as well. Traw et al. discloses that a key length or cipher type may be specified in the challenge, thus the requesting computing system must be configured (ie. capable of performing the particular key length or cipher type) to respond in the specified manner (ie. capable of the specified encryption scheme or the like).

Regarding Claim 8: The Applicant submits that Traw et al. fails to disclose features similar to those discussed in Claim 1 above.

Regarding Claims 21 and 32: The Applicant submits that Traw et al. fails to disclose features similar to those discussed in Claim 1 above.

Regarding Claims 26 and 33: The Applicant argues that Traw et al. fails to teach that any challenge requests proof that any entity is properly configured.

However, the Examiner respectfully disagrees and submits that Traw et al. does in fact disclose this feature. Traw et al. discloses that a key length or cipher type may be specified in the challenge, thus the requesting computing system must be configured(ie. capable of performing the particular key length or cipher type) to respond in the specified manner(ie. capable of the specified encryption scheme or the like) [column 5, lines 1-10 | column 7, lines 16-21].

Conclusion

11. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

Application/Control Number:
10/827,082
Art Unit: 2135

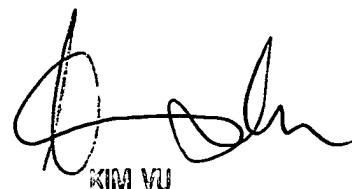
Page 13

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Edward Zee whose telephone number is (571) 270-1686. The examiner can normally be reached on Monday through Thursday 9:00AM-5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

EZ
December 17, 2007



KIM VU

USPTO PATENT EXAMINER
ELECTRONIC BUSINESS CENTER